In re Patent Application of:
MACCHETTI ET AL.
Serial No. **09/974,705**
Filed: **OCTOBER 10, 2001**

REMARKS

The Examiner is thanked for the thorough examination of the present application. The specification is being amended to delete the hyperlinks and/or other forms of browser-executable code as requested by the Examiner. Dependent Claim 25 is being amended to correct a minor informality as helpfully pointed out the Examiner. Accordingly, the indefiniteness rejection of Claim 25 is overcome.

The patentability of the claims is discussed in greater detail below. Favorable reconsideration is respectfully requested.

I. The Claimed Invention

Independent Claim 31, for example, is directed to a device for converting data between an unencrypted format and an encrypted format. The device comprises a register for storing the data in the form of bit words, and a circuit. The circuit is for performing a plurality of transformation rounds, with each transformation round comprising applying at least one transformation to a two-dimensional array of rows and columns of bit words defining a state array. Each transformation round further comprises transposing rows and columns of the state array to form a transposed state array for at least one of the transformation rounds so that at least one transformation is applied to the transposed state array. Independent Claim 21 is a method counterpart to Claim 31 and recites similar recitations. Independent Claim 44 also recites similar recitations to Claim 31, but further recites

that each transformation round also comprises applying at least one round key to the state array in at least one of the transformation rounds.

II. All The Claims Are Patentable

The Examiner rejected independent Claims 21, 31, and 44 as unpatentable over the Ohkuma et al. patent publication. The Examiner correctly notes that the Ohkuma et al. patent publication discloses an encryption device comprising a register for storing data in the form of a bit word, and a circuit for performing a plurality of transformation rounds to a two-dimensional array of rows and columns of bit words defining a state array. The Examiner incorrectly contends that the Ohkuma et al. patent publication discloses transposing row and columns of the state array. As support for this contention, the Examiner points to paragraphs [0268] - [0273] of the Ohkuma et al. patent publication. Yet paragraph [0268] merely states that "a matrix is obtained by substituting rows, substituting columns, and arbitrarily transposing in an arbitrary MDS matrix may be used".

In contrast, the above-noted independent claims recite performing a plurality of transformation rounds where each transformation round comprises transposing rows and columns of the state array to form a transposed state array. The Ohkuma et al. patent publication fails to disclose that each transformation round comprises transposing rows and columns of the state array to form a transposed state array. Instead, the above-noted text of the Ohkuma et al. patent publication merely teaches "substituting rows, substituting

columns". Further, the examples disclosed in the Ohkuma et al. patent publication, e.g. paragraphs [0262], [0263], [0265], and [0266], fail to teach that a row will be transposed with a column.

Accordingly, independent Claims 21, 31, and 44 are patentable. Their dependent claims, which recite yet further distinguishing features of the invention, are also patentable, and require no further discussion.

CONCLUSION

In view of the arguments presented above, it is submitted that all of the claims are patentable. Accordingly, a Notice of Allowance is respectfully requested in due course. Should any minor informalities need to be addressed, the Examiner is encouraged to contact the undersigned at the telephone number listed below.

Respectfully submitted,

DOUGLAS J. VISNIUS
Reg. No. 48,012
Allen, Dyer, Doppelt, Milbrath
& Gilchrist, P.A.
255 S. Orange Avenue, Suite 1401
Post Office Box 3791
Orlando, Florida 32802
407-841-2330
407-841-2343 fax
Agent for Applicants

In re Patent Application of:
MACCHETTI ET AL.
Serial No. **09/974,705**
Filed: **OCTOBER 10, 2001**

CERTIFICATE OF FACSIMILE TRANSMISSION

I HEREBY CERTIFY that the foregoing correspondence has been forwarded via facsimile number 571-273-8300 to the Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450 this 28th day of September, 2005.